PROJEKT NO MORE RANSOM: O TYM JAK 4 MILIONY OFIAR ZŁOŚLIWEGO OPROGRAMOWANIA WALCZYŁO Z HAKERAMI

Data publikacji 07.08.2020

Podczas gdy świat znalazł się w szponach epidemii koronawirusa, inny wirus po cichu sieje spustoszenie. Pomimo, iż ten wirus istnieje od lat, w ciągu ostatnich kilku miesięcy jego liczba niepokojąco wrosła i wpłynęła negatywnie na działania infrastruktury krytycznej niektórych szpitali i sparaliżowała działania wielu podmiotów.

Ten wirus to złośliwe oprogramowanie (ang. ransomware). Jednakże istnieje darmowy projekt o nazwie No More Ransom, który pomaga ofiarom przestępczości komputerowej walczyć z procederem bez płacenia hakerom.

Międzynarodowy projekt obchodzi czwartą rocznicę realizacji. W tym czasie repozytorium narzędzi deszyfrujących No More Ransom zarejestrowało od momentu jego uruchomienia ponad 4,2 miliona odwiedzających z 188 krajów i powstrzymało szacowane na blisko 632 miliony dolarów żądania wyłudzeń, które nie trafiły do kieszeni przestępców.

Oparty na wkładzie swoich 163 partnerów, portal dodał 28 narzędzi w ubiegłym roku i może teraz odszyfrować 140 różnych typów infekcji ransomware. Portal jest dostępny w 36 językach. Biuro do Walki z Cyberprzestępczością KGP jest jedym z aktywnych partnerów projektu.

Jak działa No More Ransom

No More Ransom to pierwsze tego rodzaju działanie w ramach partnerstwa publiczno-prywatnego, które pomaga ofiarom oprogramowania ransomware odzyskać zaszyfrowane dane bez konieczności płacenia kwoty okupu cyberprzestępcom.

Aby to zrobić, po prostu wejdź na stronę NO MORE RANSOM! i postępuj zgodnie z instrukcjami Crypto Sheriff, aby pomóc zidentyfikować rodzaj ransomware wpływający na urządzenie. Jeśli rozwiązanie jest dostępne, zostanie udostępniony link do bezpłatnego pobrania narzędzia deszyfrującego.

Profilaktyka jest najlepszym lekarstwem

No More Ransom pomaga ludziom dotkniętym przez oprogramowanie ransomware, niestety istnieje wciąż wiele rodzajów złośliwego oprogramowania, którego nie można pozbyć się z urządzeń. Na szczęście istnieją środki zapobiegawcze, które możesz podjąć, aby zabezpieczyć się przed oprogramowaniem ransomware:

- Zawsze przechowuj kopie najważniejszych plików w innym miejscu: w chmurze, na innym dysku w trybie offline, na karcie pamięci lub na innym komputerze.
- Używaj niezawodnego i aktualnego oprogramowania antywirusowego.
- Nie pobieraj programów z podejrzanych źródeł.
- Nie otwieraj załączników w wiadomościach e-mail od nieznanych nadawców, nawet jeśli wyglądają na ważne i wiarygodne.
- A jeśli jesteś ofiarą, nie płać okupu!

Znasz innowacyjne rozwiązanie do walki z ransomware, które mogłyby pomóc ofiarom odzyskać ich pliki bez poddawania się żądaniom przestępców, a które nie są jeszcze uwzględnione w portalu? Chętnie poznamy Twoją opinię. Nasze dane kontaktowe znajdziesz pod tym adresem.

(EUROPOL / as / dm)